protiviti
Independent Risk Consulting

711 Louisiana St.
Suite 1200
Houston, Texas 77002

General 713.314.4900
www.protiviti.com

March 31, 2005

Jonathan G. Katz, Secretary
U.S. Securities and Exchange Commission
450 Fifth Street, NW
Washington, DC 20549-0609

Re: File No. 4-497 -- Comments and Feedback on Implementation of the Sarbanes-Oxley Internal Control Provisions

We respectfully submit our comments and feedback on our experiences in the role of advisor to our clients as they evaluated the effectiveness of their internal control over financial reporting (ICFR) and formulated an assertion with respect to such ICFR in accordance with The Sarbanes-Oxley Act of 2002 (SOA), and specifically with Section 404 of the Act. While we are neither a registrant nor an accounting firm, we are offering insight arising from a multitude of experiences as an advisor to many accelerated filers and other companies and exposure to all of the major accounting firms.

We support the overall objective of SOA to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes. We believe that, as with other significant undertakings, there are opportunities to learn from first adopter experiences. Lessons learned provide the impetus for improving the efficiency and effectiveness of the compliance process to ensure that it is fair and balanced. Based on our experiences, we offer several recommendations for the Securities and Exchange Commission (SEC or Commission) to consider. Some of these recommendations may be more appropriately within the purview of the Public Company Accounting Oversight Board (PCAOB).

Our recommendations focus on the following topics:

- Clarify what constitutes “reasonable assurance”
- Increase the focus on a risk-based approach
- Increase consistency to foster improved understanding and better execution
- Clarify management’s prerogative to rely on self-assessment
- Clarify when auditors can provide advice to management around financial reporting
- Further clarify interim expectations of management

Our recommendations, along with supporting comments and feedback, are provided below.

Clarify What Constitutes “Reasonable Assurance”

Issue: There is limited guidance regarding when companies have “complied” in achieving “reasonable assurance” regarding (a) the reliability of financial reporting and (b) the adequacy of the body of evidence supporting management’s assertion in the annual internal control report. Absent such guidance, companies are effectively subject to standards written for the auditors and to the auditor's interpretations of those standards. Without a tool, management is unable to effectively gauge the effort and control the related costs.

Recommendation: Provide guidance to management as to what constitutes "reasonable assurance" when conducting the annual assessment of ICFR. Clarify what constitutes a sufficient effort in the assessment process.

Discussion: SOA Sections 404 and 302 are broad, interrelated rules focused on achieving reliability of financial reporting. Because there is limited guidance regarding when companies have "complied" in achieving reasonable assurance that financial reporting is reliable, the nature, timing and extent of management's assessment process must default to the standards written for the auditors. Guidance as to what constitutes "reasonable assurance" would provide management a foundation for understanding when sufficient documentation and an appropriate body of evidence exist to support a conclusion regarding the effectiveness of ICFR. It would also help management and auditors delineate the activities each must perform to discharge their respective responsibilities under SOA.

The goal of providing "reasonable assurance regarding the reliability of financial reporting" is embodied in both the annual internal control report required under Section 404 and the quarterly executive certification required under Section 302. The concept of reasonable assurance recognizes that a registrant can never expect to eliminate risk, and is built into the definition of ICFR adopted by the SEC in the final Section 404 rule. "Reasonable assurance" is also a long-standing principle rooted in the auditing literature, in the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control – Integrated Framework and in the Foreign Corrupt Practices Act of 1977. It is an important concept because management must attain this level of assurance when formulating a conclusion regarding the effectiveness of ICFR in achieving specific objectives or assertions around reliable financial reporting. It is intended to be a practical standard, because regardless of its design, a system of internal controls has inherent limitations. Achieving absolute assurance is a cost-prohibitive, if not an impossible, standard to achieve. That all said, very little has been added to the literature over the years as to what the "reasonable assurance" concept actually means in practice.

The compliance process should not be a bottomless pit into which registrants throw resources and money. There needs to be an articulation of the goal at a sufficiently granular level, so that management, audit committees and auditors can say, "That is enough." Absent expanded guidance, companies have limited options beyond performing their assessment consistent with the standards written for the auditors.

For example, following are among the activities a company should implement to build a credible case for achieving a reasonable level of assurance:

- Document the critical processes supporting financial reporting and the most important underlying controls embedded within those processes which provide a basis for concluding that relevant financial reporting assertions are met -- This documentation should be sufficient to enable an independent party to review it for purposes of evaluating the design effectiveness of ICFR. New employees should be able to review the documentation for their functional area to learn their roles and understand how they are expected to contribute to the control environment.

- Establish an effective process for risk identification -- Management should periodically assess the financial reporting risks inherent in the company's processes. This process should result in periodic improvements in the company's processes and in the underlying controls embedded within those processes.
- Implement a robust self-assessment process to periodically confirm that key controls remain in place -- This process should facilitate periodic feedback from process owners regarding the continued effectiveness of the most important controls in the critical processes comprising the registrant's ICFR. It should be supported by periodic testing of the most important controls by the process owners responsible for those controls. It should not be confused with the "back-up certifications" commonly used in practice.
- Provide appropriate oversight by implementing an effectively-functioning process for monitoring and testing -- This process should include independent "over testing" of process owner testing and other independent tests of controls by an objective and competent evaluator (such as an effective internal audit function). This documentation should be sufficient to enable an independent party to review it for purposes of evaluating the operating effectiveness of ICFR.
- Implement effective company-level controls that are periodically reviewed with the audit committee as changes occur in the company -- The registrant's entity-level controls, including its anti-fraud program, should be continually strengthened with the objective of improving entity-level monitoring and auditing systems that report and provide feedback with respect to the performance of the financial reporting process. This continuous improvement process should be supported through effective audit committee oversight. Management should (1) consistently enforce the code of conduct and established policies, (2) appropriately follow-up and investigate complaints around the financial reporting process, and (3) appropriately respond to any ethical or policy violations, including modification of compliance standards, policies and procedures.
- Implement a process to identify when changes in critical processes and important controls occur -- This ongoing process should monitor for and escalate change which materially affects, or is reasonably likely to materially affect, ICFR.
- Document "management's assessment process" to conclude as to the effectiveness of ICFR, in a manner sufficient that an independent party can understand what was actually done and the basis for management's conclusions -- The documentation supporting management's assessment process should provide reasonable support for the assessment, as explained in paragraph 42 of Auditing Standard No. 2 (AS2). This documentation should address the processes, procedures and due diligence management completed when executing its responsibilities and supporting its conclusions.

If the SEC were to articulate the activities necessary for management to achieve reasonable assurance for purposes of evaluating the effectiveness of ICFR, companies would have a better road map to "institutionalize" the compliance process around ICFR. With that road map as the foundation, companies can move on to improving efficiency and effectiveness.

Increase the Focus on a Risk-Based Approach

Issue: The extent of control documentation, testing and monitoring is often driven by quantitative coverage objectives, resulting in high risk areas and lower risk areas being accorded the equivalent level of effort.

Recommendation: Reaffirm that the process of evaluating ICFR is driven by a top-down, risk-based approach to ensure that the right level of effort and resources is directed to the right areas in proportion to the risk. While companies must establish a pervasive system of internal control for all aspects of their organizations, not all controls are equally significant. Nor do all accounts and assertions have the same likelihood of material misstatement. Both COSO and the PCAOB have recognized that a risk-based approach will more effectively drive the scope of an ICFR assessment. The importance of risk identification and assessment processes needs to be re-emphasized as a tool for ensuring that management, the auditors and public reports in general are focused on the most significant issues. A risk-based approach also leads to a more efficient and effective compliance process.

Discussion: If it isn't risk-based, an evaluation of ICFR is an endless process. If approached solely with a quantitative view as opposed to a top-down focus, the evaluation can lead to misguided effort and significant waste. The COSO Internal Control – Integrated Framework and the PCAOB's Auditing Standard No.2 provide for a risk assessment to drive management's assessment process. A risk-based approach is the most practical way to evaluate ICFR because it ensures a sharper focus when (1) determining the nature and extent of process documentation, (2) the selection of controls to evaluate and test, and (3) the nature, timing and extent of controls testing. Simply stated, a risk-based approach ensures that the assessment process sufficiently addresses the right things.

In a process as intricate as an evaluation of the effectiveness of ICFR, a continuous improvement mindset can help eliminate non-essential practices and simplify and focus the process. Based on our experience, following are a few examples of areas that should be reviewed by management and the auditors with the intent of applying a truly risk-based approach:

- There needs to be an assessment of the level of effort required to test routine transactions. Testing to the same extent every account above a quantitative threshold, without regard to the relative risk, is driving excessive work. A quantitative approach to the scoping process often allocates a significant testing effort to controls over routine transaction processing areas, even though the history of past financial reporting scandals has shown that the real financial reporting risks often lie within such areas as non-routine transaction processing, estimation transaction processing, complex reporting and disclosure requirements, and the potential for management override of established processes and controls. Despite this anomaly, extensive detailed testing is often performed in areas where the risk of material error is low.

- There needs to be an evaluation as to whether the right level of effort and resources is being directed to the right areas. For example, more emphasis should be directed to evaluating the effectiveness of entity-level controls, antifraud controls, the period-end financial reporting process and other areas, including audit committee oversight, in proportion to the relative risk, consistent with a risk-based approach. The effort expended in these areas should be greater in proportion to the total effort. To illustrate:
  - Despite the vital importance to reliable financial reporting, the "softness" of entity level controls and the antifraud program and related controls often led evaluators to place greater weight on performing more testing of the "more tangible" controls over routine processes. While this practice creates an impressive body of work, it drives up the cost of the evaluation process with diminishing returns. For example, the process of documenting, evaluating and testing the controls over prepaid assets and intercompany accounts may not be nearly as important as testing the controls to prevent, deter and detect fraud in sensitive areas.
  - The emphasis given to controls over information technology (IT) affecting financial reporting processes was oftentimes less in relation to manual process controls. For example, increased attention needs to be given to understanding IT-related risks and to integrating the testing of IT application controls and manual controls at the process level, including IT application controls embedded within ERP systems. There also needs to be a sharper focus on IT general controls and how they affect the evaluation of controls over key IT applications. For example, these controls include (1) IT application-level user access controls, including controls over IT application segregation of duties requirements and (2) other IT general controls, including the consideration of change controls. If management is able to conclude on the effectiveness of IT general controls, the scope of tests over IT application controls can be appropriately focused.
- A truly risk-based evaluation should drive the selection of controls to test. Our experience indicates there is significant variability among both companies and auditors when it comes to selecting the controls to test. The filtering process is vital to making the assessment of ICFR more efficient and effective, because it narrows down the population of controls to the ones that really matter, making the linkage of individual controls with the significant accounts and assertions to which they relate, as required by paragraph 84 of AS2, a more manageable task. Filtering also increases the efficiency of testing, because excessive testing drives significant non-value-added activity around controls that aren't that important to the overall assessment of ICFR.

The SEC and PCAOB should reaffirm that the process of evaluating ICFR must be driven by a top-down, risk-based approach that directs the appropriate level of effort and resources to the right areas in proportion to the risk. If management is able to formulate a conclusion around the key risks, and the auditor is able to concur with that conclusion early in the process, the ICFR assessment is less likely to meander.

Increase Consistency to Foster Improved Understanding and Better Execution

Issue: The complexities of the ICFR evaluation process led to inconsistencies and variations in many areas. Leaving the resolution of these inconsistencies and variations to be sorted out in the marketplace can lead to a "lowest common denominator" approach.

Recommendation: More consistency is needed with respect to critical steps in the ICFR assessment process. Increased consistency will foster improved understanding as well as more efficient and effective execution by both management and auditors. Therefore:

- Facilitate an effort to streamline the process and reduce inconsistencies. (The Commission's April 13 meeting should be an excellent first step.)
- Accumulate case studies and examples and provide further guidance as to what is and what isn't a material weakness.
- Review application of the so-called "Nine Firm Framework" in practice for purposes of evaluating whether more granular guidance of the process outlined in AS2 for assessing and aggregating control deficiencies is needed.

Discussion: The guidance for the ICFR assessment process is primarily found in AS2, which is directed to auditors. That guidance is largely principles-based. As discussed earlier in this letter, management of many companies had to react to the auditor's requirements because they had no other place to which to turn. The complexities of the process and the number of decision points during the process led to inconsistencies and variations in many areas in practice. That should be no surprise, because there are many areas in which reasonable men and women can differ in exercising judgment. This makes an already difficult project even tougher to execute. To illustrate,

- There is significant variability among different audit teams around the application of an "account coverage test" for purposes of determining the extent of coverage of a material account by the locations and units comprising a "large portion" of the company's operations and financial position. If the coverage wasn't sufficient, the auditor required selection of more units and locations to test. We experienced "account coverage" requirements ranging from 50 percent to as high as 95 percent.
- While the principles underlying it are not new, the process of classifying and aggregating control deficiencies has never been applied before on such a broad scale by so many companies and auditors. Many of our first-adopter clients were of the view that the thought process around determining the severity of control deficiencies was somewhat mechanical in application and the approach to aggregating multiple deficiencies was arbitrary. The process of classifying deficiencies can be complex and time-consuming. Part of this difficulty arose from applying a rigorous decision model to a wide variety of different company circumstances. That model is "A Framework for Evaluating Control

Exceptions and Deficiencies" developed by representatives of nine accounting firms as a supplement to the guidance in AS2 (the "Nine Firm Framework").

- The extent to which the auditor uses the work of others, particularly on the work of an effective internal audit function, and the process by which the auditor evaluates that work, has varied widely in practice. The process by which the auditor evaluates the persons performing work has also varied in practice, sometimes straying beyond the criteria specified in paragraphs 119 and 120 of AS2.

In addition to the above examples, we noted inconsistencies and variations with respect to the following activities:

SETTING THE FOUNDATION, ASSESSING CURRENT STATE AND IDENTIFYING RELEVANT PROCESSES

- Determining planning materiality
- Executing the scoping approach to:
  - Selecting priority financial reporting elements
  - Selecting priority processes
  - Selecting priority application systems
  - Achieving coverage of significant units and locations

DOCUMENT DESIGN EFFECTIVENESS

- Executing the approach to performing walkthroughs
- Executing the approach to "baselining" IT controls
- Considering applicability of the COSO components at both the entity and process levels
- Determining the nature and extent of internal control design documentation
- Considering the extent and depth of emphasis on selected controls
  - Company-level controls
  - IT application-level user access controls, including controls over cross-IT application segregation of duties requirements
  - Other IT general controls, including the consideration of change controls
  - Antifraud program and related controls
  - IT application controls when ERP systems are in place
  - Controls over spreadsheets
  - Controls over routine processes
  - Controls over non-routine processes and estimation transactions
  - Controls over the period-end financial reporting process

TEST OPERATING EFFECTIVENESS

- Selecting the critical controls to test
- Selecting sample sizes for tests of manual controls
- Selecting sample sizes for tests of automated controls
- Applying sampling methods to different situations, i.e., monthly account reconciliations
- Testing of controls around and embedded within ERP systems

- Evaluating the need and timing for SAS 70 letters
- Determining the minimum periods during which controls must operate to be tested for operational effectiveness, affecting the acceptance of retests of remediated controls
- Determining the nature, timing and extent of refresh testing
- Determining the nature and extent of documentation required to evidence the execution of individual controls
- Determining the nature and extent of documentation required to support controls testing
- Assessing the nature, timing and extent of independent testing of controls, given the existence of an effectively-functioning process-owner self-assessment program (see separate point below)

With respect to the above variations and inconsistencies, we recommend the following:

(1) Notwithstanding that variations and inconsistencies tend to sort themselves out over time, the PCAOB should facilitate an effort to streamline the evaluation process and reduce inconsistencies, leading to a more cost-effective approach. Permitting a market-driven resolution would likely result in an evolution toward the least intrusive standard, rather than a standard that best serves the public interest.

(2) Examples from first-year-filer situations should be accumulated to further the depth of understanding as to how the severity and likelihood of control deficiencies were assessed, classified and aggregated. The PCAOB should review the application of the Nine Firm Framework in light of the examples collected and consider issuance of further guidance to supplement the direction in AS2.

Understanding variability in practice in significant activities and evaluating the need for additional guidance to narrow the range of variability will foster greater understanding and more efficient and effective execution of the ICFR assessment process by both management and auditors.

Clarify Management's Prerogative to Rely on Self-Assessment

<u>Issue</u>: <u>When evaluating the sufficiency of management's assessment process</u>, auditors may not recognize an effectively-functioning self-assessment program as evidential matter. As a result, auditors may require management to perform the same level of independent controls testing as if there were no self-assessment program in place,

<u>Recommendation</u>: Explicitly acknowledge that if management relies on self-assessment when accumulating the body of evidence for purposes of concluding as to the effectiveness of ICFR, such reliance may result in appropriate reductions in the nature, timing and extent of the independent testing required during the assessment process to support management's conclusions.

<u>Discussion</u>: Going forward, many registrants will use self-assessment as <u>one</u> source of evidence in supporting management's assertion regarding the effectiveness of ICFR. The term, "self-assessment", is often used to describe circumstances where process owners evaluate the controls for which they are responsible and communicate the results of their self-review to management. A robust self-assessment approach is always process-based, and involves several key components, including the (a) identification of the most important controls, (b) identification of the owners of those controls, (c) predetermination of questions approved by management, (d) rigorous deployment of questions and appropriate follow-up with owners, and (e) resolution of exceptions and open matters on a timely basis. Self-assessment may be enhanced to a higher form of evidence if process owners are required to test a minimum sample of items before formulating their assessments of certain controls. These self-applied tests augment the inquiry, observation and inspection techniques process owners often use as they supervise and monitor the activities for which they are responsible on a day-to-day basis to assess whether controls are functioning properly.

Self-assessment should be an integral part of the body of evidence arising from management's assessment process. Accordingly, management should receive credit from the external auditor for using self-assessments when the auditor evaluates the sufficiency of the evidence supporting <u>management's</u> assessment process. We believe that the substance of paragraphs 40, 53 and 126 of AS2 provides guidance on this point. However, we are not convinced it is generally understood that the use of self-assessment can lead management to conclude that a reduction in the nature, timing and extent of independent testing is appropriate. There are three reasons why:

(1) As pointed out earlier in our letter, there is no authoritative statement directed to management specifying general principles around the execution of the assessment process.

(2) There are many instances in practice where external auditors are applying an "as much or more" principle to their evaluation of management's independent controls testing relative to their own testing in performing an audit of ICFR. In other words, the testing performed by competent and objective evaluators (which, under AS2, would not include self-assessments and testing by process owners) must be as much or more than the testing the auditor will perform. Since the auditor is not allowed to rely on self-assessment as prescribed by AS2, they are by default not giving credit to management for self-assessment activity.

(3) The PCAOB's guidance, as noted in paragraph 126 of AS2, acknowledges that management may test the operating effectiveness of ICFR using a self-assessment process. That guidance uses the direction provided in paragraphs 120 through 125 to assert that the auditor may not use this work. However, it is not clearly stated in AS2 that auditors should not construe the restrictive direction provided them by the Board as also applying to management.

Consistent with a principles-based approach, the PCAOB should explicitly acknowledge that the use of self assessment, as defined herein, by management can reduce the nature, timing and extent of independent controls testing required to support management's assessment process.

Clarify When Auditors Can Provide Advice to Management around Financial Reporting

Issue: Companies are finding it more difficult to use the expertise they need to interpret increasingly complex accounting and reporting rules and apply those rules to a constantly changing business environment.

Recommendation: Assess whether the current application of the independence rules is preventing constructive dialogue between companies and their auditors around the application of the accounting rules and determine whether modifications are needed.

Discussion: We have observed a number of instances where the dynamic of the client-auditor relationship has changed such that the interactive process related to financial reporting is significantly affected. While this result may be intended from a public policy standpoint, it is our experience that many companies are of the view that they are not receiving timely access to the financial reporting expertise they believe is needed to properly apply accounting principles -- particularly in highly complex accounting and reporting areas. The application of the independence requirements on public accounting firms is dictating this result.

When evaluating whether this end result is the desired one, it is important to recognize that there aren't many advisors in financial accounting and reporting matters available to companies, outside of the major accounting firms. Even the most seasoned accountants must cross-check their accounting and reporting judgments. No one should be surprised when even the most savvy and financial-reporting-wise CFO feels a need to discuss his or her company's accounting and reporting with an expert who follows the development of the related rules on a full-time, day-to-day basis. In today's environment, we are seeing many situations where the CFO reaches out to the expertise of the external audit firm for advice, but finds the firm unwilling to engage for fear that they may impair their independence. The CFO is instructed to determine the answer and then subject it to the audit process. Since few companies have in-house expertise that is fully versed on all of the intricacies of complex accounting matters, the CFO does not feel adequately equipped to develop the correct interpretation without access to appropriate expertise. Further, he or she does not feel comfortable he or she can reach out to another accounting firm because of the risk of being perceived as opinion shopping. If the company uses two accounting firms in the audit process, the consultation options are further reduced. This exercise leaves well-intended financial management in a quandary.

We have also seen on a more limited basis, situations where the company draws its conclusion on the appropriate accounting, presents its preliminary conclusions to its auditors, and through this process discovers it either misinterpreted GAAP or missed existing literature available on the subject matter. The accounting firm presents this new information and informs the company that its initial conclusions were incorrect. Both sides agree and the company changes its proposed accounting policy prior to publishing its financial statements. However, since management did not reach the correct conclusion in its initial effort, the auditing firm believes it needs to evaluate this event as a significant deficiency in its internal control due to lack of sufficient accounting talent within the company.

The irony of the current environment is that companies are finding it more difficult to use the very expertise they need to interpret increasingly complex accounting and reporting rules and apply those rules to a constantly changing business environment. While we are in complete agreement with the importance of maintaining auditor independence in both fact and appearance, we are not satisfied that the environment described above is practical or in the public interest, either now or in the future, and suggest that it be evaluated to determine whether a more constructive approach is possible.

Further Clarify Interim Expectations of Management

Issue: There is potential for confusion regarding the overlap between disclosure controls and procedures (DCP) and ICFR and the related questions around the responsibility of certifying officers' to assess ICFR on a more frequent than annual basis. Therefore, certifying officers may be exposed to enforcement and other actions when honest mistakes occur.

Recommendation: Additional clarity is needed around management's responsibility to evaluate ICFR on a more frequent than annual basis. The SEC should either narrow its definition of DCP or clarify its expectations of certifying officers as to their responsibility to evaluate ICFR.

Discussion: A quarterly evaluation of DCP continues to be required under Section 302 and many elements of ICFR are, as noted by the Commission, "subsumed" by DCP. In our comment letter to the SEC dated November 26, 2002 on the proposed Section 404 rule, we noted that there appears to be a de facto requirement to evaluate ICFR on an interim basis. In finalizing its Section 404 rule, the Commission addressed this issue by, among other things, pointing out that "in designing their disclosure controls and procedures, companies can be expected to make judgments regarding the processes on which they will rely to meet applicable requirements." Notwithstanding the Commission's efforts to provide clarity, further clarity is needed around management's responsibility to evaluate ICFR on a more frequent than annual basis.

The Commission's definition of DCP is a very broad one, by any standard. It is so broad, it encompasses an overwhelming portion of the total population of controls comprising ICFR. The Commission should either narrow its definition of DCP or clarify its expectations of certifying officers as to their responsibility to evaluate ICFR. In submitting this recommendation, we wish to make it very clear that we do not advocate any extension of the current Section 404 rule beyond the present annual assessment requirement mandated by SOA.

This matter has public policy implications. Restatements are going to occur in the future. Regulators can expect that honest mistakes will be made. The complexities of the financial reporting model will continue to lead to misapplications and disagreements over the proper accounting for specific transactions. Reasonable men and women are going to disagree when applying the financial accounting rules to new and complex situations. More importantly, there are the inherent limitations in any internal control system we discussed earlier in this letter. Human judgments in decision-making, breakdowns due to human error and simple mistakes can arise over time.

The public policy risk is that the overlap between DCP and ICFR can result in well-intentioned people being exposed to enforcement and other actions when honest mistakes occur, because of confusion as to whether certifying officers should be assessing ICFR on a more frequent than annual basis. Therefore, to make SOA and the compliance process fairer and enable certifying officers to avoid "double jeopardy", the Commission should either narrow the definition of DCP to more effectively delineate them from ICFR or, alternatively, further clarify its expectations of certifying officers.

We appreciate the opportunity to submit our comments and feedback. We hope they are helpful to the Commission and to its staff. If the staff would like to discuss any of the points made in this letter, please contact Jim DeLoach at (713) 314-4981.

Very truly yours,

Protiviti Inc.

By: James W. DeLoach, Jr.
Managing Director